PATENT ABSTRACTS OF JAPAN

(11)Publication number : 2001-136159

(43)Date of publication of application : 18.05.2001

---

(51)Int.Cl. H04L 9/08
H04B 7/24
H04H 1/00
H04N 7/173

---

(21)Application number : 11-311651 (71)Applicant : SONY CORP

(22)Date of filing : 01.11.1999 (72)Inventor : AKACHI MASAMITSU

---

(54) INFORMATION TRANSMISSION SYSTEM AND METHOD, TRANSMITTER AND RECEIVER

(57)Abstract:

PROBLEM TO BE SOLVED: To obtain an information transmission system that can conduct various reception controls.

SOLUTION: In the case of transmitting data individually to receivers, the data including an address specific to a concerned receiver are transmitted, and in the case of transmitting common data to receiver of an optional group, common address information denoting a common address among the receivers of the optional group and address range information designating the range of the common part of the address are attached to the data and the resulting data are transmitted. The receiver receivers the transmitted data and decodes the transmitted data when the specific address is coincident with the address attached to the data or when the specific

address is compared with the common address information attached to the data within a range denoted by the address range information and the result of comparison indicates coincidence.

CLAIMS

[Claim(s)]
[Claim 1]In an information transmission system which transmits data to two or more receiving sets which have a respectively peculiar address via a predetermined transmission line from a sending set, When transmitting data individually to the above-mentioned receiving set, while giving an address peculiar to the receiving set concerned to the data concerned and transmitting, When transmitting common data to arbitrary groups' above-mentioned receiving set, Common address information showing an intersection of the above-mentioned address which is common between the above-mentioned receiving sets of a group of the above-mentioned arbitration, When the above-mentioned sending set which gives address range information which specifies the range of an intersection of the address concerned to the data concerned, and transmits, and the above-mentioned data are received and the peculiar above-mentioned address and the above-mentioned address given to the data concerned are in agreement, Or an information transmission system having the above-mentioned receiving set which decodes the above-mentioned data when it compares in the range the above-mentioned address range information indicates the peculiar above-mentioned address and the above-mentioned common address information given to the data concerned to be and a comparison result is in agreement.
[Claim 2]When transmitting data to two or more above-mentioned above-mentioned receiving sets of all, give, transmit the above-mentioned sending set to the above-mentioned data by making a predetermined multiple address address into the above-mentioned common address information, and the above-mentioned receiving

set, The information transmission system according to claim 1 characterized by decoding the data concerned when the above-mentioned multiple address address is given to the received above-mentioned data.

[Claim 3]The information transmission system according to claim 1 the above-mentioned receiving set's changing the above-mentioned address into an address of the smaller number of bits, and performing comparison with the peculiar above-mentioned address and the above-mentioned address given to the above-mentioned data using the changed address concerned.

[Claim 4]When the above-mentioned sending set's transmitting data individually to the above-mentioned receiving set, while enciphering the data concerned using a secret key corresponding to the above-mentioned address peculiar to the receiving set concerned, When transmitting common data to between arbitrary groups' above-mentioned receiving sets, encipher using a predetermined common key and the data concerned the above-mentioned receiving set, While decoding data individually transmitted to the receiving set concerned using a secret key corresponding to the above-mentioned address peculiar to the receiving set concerned, The information transmission system according to claim 1 decoding data transmitted to between arbitrary groups' above-mentioned receiving sets using the above-mentioned common key.

[Claim 5]In an information transmission method which transmits data to two or more receiving sets which have a respectively peculiar address via a predetermined transmission line from a sending set, When transmitting data individually to the above-mentioned receiving set, while giving an address peculiar to the receiving set concerned to the data concerned and transmitting, When transmitting common data to arbitrary groups' above-mentioned receiving set, Common address information showing an intersection of the above-mentioned address which is common between the above-mentioned receiving sets of a group of the above-mentioned arbitration, When a transmission step which gives address range information which specifies the range of an intersection of the address concerned to the data concerned, and transmits, and the above-mentioned data are received and the peculiar above-mentioned address and the above-mentioned address given to the data concerned are in agreement, Or an information transmission method having a receiving step which decodes the above-mentioned data when it compares in the range the above-mentioned address range information indicates the peculiar above-mentioned address and the above-mentioned common address information given to the data concerned to be and a comparison result is in agreement.

[Claim 6]When transmitting data individually to the above-mentioned receiving set in a sending set which transmits data to two or more receiving sets which have a respectively peculiar address, while giving an address peculiar to the receiving set concerned to the data concerned and transmitting, When transmitting common data

to arbitrary groups' above-mentioned receiving set, A sending set giving common address information showing an intersection of the above-mentioned address which is common between the above-mentioned receiving sets of a group of the above-mentioned arbitration, and address range information which specifies the range of an intersection of the address concerned to the data concerned, and transmitting.

[Claim 7]The sending set according to claim 6 giving and transmitting to the above-mentioned data by making a predetermined multiple address address into the above-mentioned common address information when transmitting the above-mentioned data to two or more above-mentioned above-mentioned receiving sets of all.

[Claim 8]When transmitting the above-mentioned data individually to the above-mentioned receiving set, while enciphering the data concerned using a secret key corresponding to the above-mentioned address peculiar to the receiving set concerned, The sending set according to claim 6 characterized by enciphering the data concerned using a predetermined common key when transmitting common data to between arbitrary groups' above-mentioned receiving sets.

[Claim 9]When an address given to the received above-mentioned data in a receiving set which receives and decodes data transmitted from a predetermined sending set, and an address peculiar to the receiving set concerned are in agreement, Or based on address range information which specifies common address information showing an intersection of the above-mentioned address which is common among two or more above-mentioned receiving sets given to the received above-mentioned data, and the range of an intersection of the address concerned, A receiving set characterized by decoding the above-mentioned data when the peculiar above-mentioned address is compared with the above-mentioned common address information given to the data concerned in the range which the above-mentioned address range information shows and a comparison result is in agreement.

[Claim 10]The receiving set according to claim 9 characterized by decoding the data concerned when a predetermined multiple address address is given to the received above-mentioned data.

[Claim 11]The receiving set according to claim 9 changing the above-mentioned address into an address of the smaller number of bits, and performing comparison with the peculiar above-mentioned address and the above-mentioned address given to the above-mentioned data using the changed address concerned.

DETAILED DESCRIPTION

[Detailed Description of the Invention]

[0001]

[Field of the Invention]This invention is applied to the information transmission system which transmits information via a satellite, concerning an information transmission system and a method, a sending set, and a receiving set, and is preferred.

[0002]

[Description of the Prior Art]In the digital satellite broadcasting system, the limited reception mechanism (CA:Conditional Access) in which only the just addressee who performed the receiving contract can receive broadcast is used conventionally.

[0003]In this limited reception mechanism, the predetermined secret key is beforehand passed to the addressee who performed the receiving contract. The transmitting side enciphers broadcast data using this secret key, and transmits via a broadcasting satellite. And by canceling encryption of a received wave using a secret key, the addressee is made as [listen / only the addressee who performed the receiving contract / to broadcast / view and].

[0004]

[Problem(s) to be Solved by the Invention]The satellite data transmission systems which perform data communications using a digital satellite broadcasting system are considered here in recent years. Since the transmission speed of satellite connection is quick compared with a telephone line, an ISDN circuit, etc., large capacity data can be transmitted in a short time, and there is flume ******.

[0005]The individual communication which transmits individual data to each addressee in these satellite data transmission systems. (This is hereafter called a unicast) To things, in addition, the simultaneous transmissive communication which transmits the same data to all the addressees. (This is hereafter called broadcasting) If various reception controls, such as group communication (this is hereafter called multicasting) which transmits the same data to arbitrary addressee groups, can be performed, the user-friendliness of satellite data transmission systems will be considered to improve further.

[0006]However, in the limited reception mechanism to apply, since it designed as a premise that all the addressees receive, view and listen to the always same information, there was a problem that reception controls, such as a unicast and multicasting, could not be performed.

[0007]This invention was made in consideration of the above point, and tends to propose the information transmission system and the method, sending set, and receiving set which can perform various reception controls.

[0008]

[Means for Solving the Problem]In [in order to solve this technical problem] this invention, In an information transmission method which transmits data to two or more receiving sets which have a respectively peculiar address via a predetermined transmission line from a sending set, When transmitting data individually to a receiving

set, while giving an address peculiar to the receiving set concerned to the data concerned and transmitting, Common address information which expresses an intersection of an address which is common between receiving sets of the arbitrary groups concerned when transmitting common data to arbitrary groups' receiving set, While giving address range information which specifies the range of an intersection of the address concerned to the data concerned and transmitting, Transmitted data was received, and the data concerned was decoded, when a peculiar address and an address given to the data concerned were in agreement, or when a peculiar address was compared with common address information given to the data concerned in the range which address range information shows and a comparison result was in agreement.

[0009]Common address information which expresses an intersection of an address which is common between receiving sets of the arbitrary groups concerned when transmitting common data to arbitrary groups' receiving set, Give address range information which specifies the range of an intersection of the address concerned to the data concerned, and it transmits, In a receiving set, a peculiar address is compared with common address information given to the data concerned in the range which address range information shows, and when a comparison result is in agreement, simple composition can perform various reception controls by having decoded the data concerned.

[0010]

[Embodiment of the Invention]The 1 embodiment of this invention is explained in full detail about a drawing below.

[0011](1) In entire configuration drawing 1 of satellite data transmission systems, 1 shows the satellite data transmission systems which applied this invention as a whole, and comprises the transmitting side system 2, the satellite 3, and the receiving system 4 that becomes by two or more identical configurations. The transmitting side system 2 and each receiving system 4 are connected via the Internet 5, respectively. Between the service provider which manages the transmitting side system 2, and the addressee who owns each receiving system 4, the service contract about the satellite data transmission systems 1 concerned is made beforehand.

[0012]In the transmitting side system 2, the control device 10, the digital service unit 11, the data server 12, and the transmitting processing unit 13 which control the transmitting side system 2 whole concerned are connected via the local network 14.

[0013]The control device 10 receives the data read-out demand transmitted from the information processor 22 which the receiving side device 4 has via the digital service unit 11. And according to a data read-out demand, the control device 10 reads data from the data server 12 or the data server (not shown) on the Internet 5, and supplies it to the transmitting processing unit 13.

[0014]The MAC (Media Access Control: media access control) address whose

transmitting processing unit 13 is the peculiar identification number given to each information processor 22 of the receiving side device 4 here, It has the encryption key conversion table which described the secret key set up corresponding to the MAC Address concerned. And the transmitting processing unit 13 enciphers data using the secret key corresponding to the MAC Address of the information processor 22 of the data transmission point for the data read based on the secret key conversion table. About the data transmitted to all the information processors 22 as broadcasting, the transmitting processing unit 13 is enciphered using a predetermined common key while setting the value of CKI (Common Key Indicator, after-mentioned) of the data concerned to "0." And the transmitting processing unit 13 packet-izes the enciphered data in the form provided in DVB (Digital Video Broadcasting) data-broadcasting specification, and transmits to the satellite 3 via the transmission 15 as the uplink wave S2.

[0015]The satellite 3 receives and amplifies the uplink wave S2, and broadcasts it again towards the terrestrial receiving system 4 as the down-link wave S3.

[0016]In the receiving system 4, the receiving set 21, the digital service unit 23, and two or more information processors 22 that become, for example with a personal computer etc. are mutually connected via the local network 24.

[0017]By performing decoding processing which is recovery-processed and is later mentioned to the down-link wave S3 which received via the receiving antenna 20, the receiving set 21 decodes the data transmitted towards the information processor 22, and supplies it to the information processor 22 concerned via the local network 24.

[0018]The information processor 22 will transmit the read-out demand of data to the transmitting side system 2 via the digital service unit 23 and the Internet 5 according to this, if read-out demand operation of data is inputted by the user.

[0019](2) Explain the composition of a receiving set, next the receiving set 21 of the receiving system 4 using drawing 2.

[0020]In the receiving set 21, to CPU(CentralProssecing Unit) 30 which controls the receiving set 21 whole concerned. The front end section 31, the separation part 32, the receiving filter 33, the decoding part 34, the checker 35, the buffer 36, the key table 37, and the interface part 38 are connected via the bus 39.

[0021]The front end section 31 restores to the down-link wave S3 which received via the receiving antenna 39, and supplies it to the demultiplexer 32 as the data stream D31. Based on PID (Packet ID), the demultiplexer 32 separates only a required packet from the data stream D31, and supplies it to the receiving filter 33. The receiving filter 33 investigates the contents of a pay load of the packet supplied from the demultiplexer 32, and cancels an unnecessary packet to data decryption processing.

[0022]The decoding part 34 operates based on the decoding processing mentioned later, uses the MAC Address of the information processor 22 (drawing 1) as a search key, asks the key table 28, and acquires a decode key from the key table 28

concerned. And the decoding part 34 decodes the data stream D31 using the acquired decode key, and supplies it to the checker 35 as the decode data D34.

[0023]The checker 35 inspects whether decoding processing was normally performed to the decode data D34, and supplies only the packet decoded normally to the buffer 36. And the buffer 36 reads the decode data D34 to the interface part 38 via the bus 39 according to the demand of CPU30. The interface part 38 supplies the decode data D34 to the information processor 22 via the local network 24 (drawing 1).

[0024]In this way, the receiving set 21 receives the down-link wave S3, takes out only the data supplied for turning information processor 22, and supplies it to the information processor 22 concerned.

[0025](3) The decoding processing digital stream D31 of a digital stream, As shown in drawing 3, while packet header information is added to the head of a pay load, Stuffing bytes (invalid byte) and CRC (Cyclic Redundancy Code : cyclic redundancy code) are added to the end of a pay load, It is encapsulated and constituted by the gestalt (Datagram-section) which can be processed as a session provided in DVB-data broadcast specification. The byte (8 bits) containing Bit7 to Bit0 when the most significant bit of a MAC Address is set to MAC Address #6 and Bit47 and a least significant bit are set to Bit0 here is meant.

[0026]In the decoding part 34, it discriminates from whether the packet concerned should be received based on the MAC Address and the key table 37 which were described by each packet of the data stream D31 which received first.

[0027]In this packet discrimination process here the receiving set 21 by this invention, The mask-bit processing which specifies the bit position in a MAC Address which should be compared, A MAC Address is changed into the numerical value of the smaller number of bits, and the MAC Address conversion process which discriminates from a packet using this, and MAC Address passage processing in which the packet which has a specific MAC Address is passed unconditionally are performed.

[0028]mask-bit processing adding the AND operation of a mask bit and a comparison-operation result to the state judging by the comparison operation of the MAC Address described by the section header and the MAC Address of the key table 37, coming out, and, Supposing it expresses exclusive OR with ^, it expresses a logical product with & and it expresses [a MAC Address given in a session header] the dignity of MAC (k) and a bit for MR and the MAC Address of the key table No. k-ths as I, it is for every bit. [0029]

[Equation 1]

$$(\sim (MR_I \hat{} MAC_I (k))) \& MASK_I (k) \quad \cdots\cdots (1)$$

[0030]0 <=I<=47, it carries out to all the bits in the becoming range, and the becoming operation is done for the MAC Address to have agreed, when the whole of this result is "0."

[0031]This, i.e., a mask, means that comparison of MR and a MAC Address is performed only in the bit which is "1", and there is. A relation with the comparison operation of this mask bit, MR, and a MAC Address is shown in drawing 4.

[0032]In the case of drawing 4, as for a mask bit, even D0-D3 are "0", and D4-D47 are "1." In the section of D4-D47 whose mask bit is "1" when comparing a MAC Address using this mask bit, It may be the agreement conditions of a MAC Address that a MAC Address and MR are the same, and the section of D0-D3 whose mask bit is "0" may not have a MAC Address and same MR. Thus, by comparing a part of MAC Address using a mask bit, multicasting (group communication) which distributes the same packet to the arbitrary information processors 22 which have a MAC Address different, respectively can be performed. By making all mask bits into "1", i.e., "0xFFFFFFFFFFFF", collation is performed to bits of all MAC Addresses, and a unicast (individual communication) can be performed.

[0033]Here, when performing multicasting using a mask bit, it will be the requisite that an intersection exists in a MAC Address of each information processor 22, but it is difficult to arrange the information processor 22 such, and also becomes lacking adaptability at the time of employing a system. In this case, what is necessary is to rewrite a packet header and just to make an intersection of a MAC Address in false based on a conversion table of a MAC Address of the actual information processor 22, and a MAC Address described by packet header.

[0034]A MAC Address conversion process performs an operation by a formula (hash function) of a certain kind to an inputted MAC Address, acquires a numerical value reduced to the number of bits of 48 bits or less, and searches a table (hash table) which described whether this would be made into a key and would be passed. Reduction of this number of bits is for making a hash table small. If a hash function is a function which often distributes a MAC Address inputted, anything, it will be good, for example, will calculate CRC of a MAC Address, it sets these top 6 bits to p, if Pass (p) is "1", it will make it pass, for example, if it is "0", it will be canceled. pass is a 2^6=64 bit table here. Thus, by reducing the number of bits of a MAC Address using a hash function, circuit structure of the decoding part 34 can be made small.

[0035]When MAC Address passage processing is an address for simultaneous transmissive communication predetermined in a MAC Address described by header of a packet, It says that it is not concerned with a state of a key table, but makes it pass, and if a MAC Address of a packet given in a header is "0xFFFFFFFFFFFF" (this address is called a broadcast address), it will always be regarded as simultaneous transmissive communication (broadcasting), and this will be passed. In this invention, this MAC Address passage processing is preceded with mask-bit processing and a MAC Address conversion process, and is performed. When a MAC Address given in a packet header is a broadcast address by this, search of a key table becomes unnecessary, and it is effective in processing speed improving.

[0036]The decoding part 34 discriminates from a packet based on a MAC Address described by header of a packet, a MAC Address of the information processor 21, and a mask bit in this way.

[0037]Then, the decoding part 34 detects whether a packet from which it was discriminated is enciphered. And when a packet is enciphered, a decode key is picked out from a key table and decoding processing is performed, but it is necessary to provide a common key which is a decode key shared by two or more MAC Addresses in simultaneous transmissive communication.

[0038]In the receiving set 21 by this invention, it is judged, for example using the most significant bit (D7 of the 2nd byte of the 2nd line of drawing 3) of the 6th byte of section whether a common key is used. This is called CKI (Common KeyIndicator) by this invention. And an individual key which will be extracted from a key table by MR, a MAC Address, and mask bit if CKI is "1" is used, and if CKI is "0", it will be determined that a common key is used irrespective of setting out of a key table. "1" is to set CKI to reserved in DVB-data broadcast specification, and to be taken as a value here. Since it is thought that a common key is a more nearly special disposal method compared with an individual key, it can be in agreement in specification with DVB-data broadcast specification by determining that a common key is used, when CKI is "0."

[0039]Although it may prepare a specific storage area, since processing can be communalized with an individual key and the common key can also use a storage area effectively if data of a specific line in a key table is made to serve a double purpose, it is more desirable. A top line, i.e., the 1st line, is more preferably specified as this specific line. the number n of lines of a key table -- how many -- be -- since the 1st line certainly exists, memory or extraction of a common key can be performed, without changing procedure, even if it will be a receiving set with which values of n differ, if it does in this way.

[0040]Drawing 5 shows composition of a key table and MAC Address #1 a MAC Address described by the No. 1 line of a key table, Mask #1 means key data of Even/Odd in which K_{1Even} and K_{1Odd} were able to match respectively a mask bit corresponding to MAC Address #1 with MAC Address #1, and it has bit width m according to code form to be used. A key table has two or more (n pieces) the same structures as the above. A maximum is determined from circuit structure in which the key table 28 can have this maximum number.

[0041]A MAC Address and key data have the independent Valid flag, respectively, and are made as [manage / whether a value is individually effective or invalid / it / by this], and it also becomes possible to divert the Valid flag concerned to MAC Address discrimination. Since a key table has the Valid flag which became independent for every line, The null line (invalid line) may be included, and the key table concerned should just only set a Valid bit of a MAC Address to "0" and is preferred because of high-speed processing to repeal information on a specific line temporarily by this.

[0042]The decoding part 34 decodes a packet using a decode key obtained in this way.
[0043](4) While a decoding processing procedure, next a decoding processing procedure of a digital stream are shown in a flow chart of drawing 6, explain.
[0044]The decoding part 34 starts processing by RT1, reads into the register MR the 48-bit MAC Address described by packet header in step SP1, and follows it to the following step SP2.
[0045]In step SP2, it is judged whether the decoding part 34 has a value of the register MR equal to a broadcast address (0xFFFFFFFFFFFF). When an affirmation result is obtained in step SP2, this has a value of the register MR equal to a broadcast address, Namely, it expresses that the packet concerned is a broadcasting packet, and the decoding part 34 skips Steps SP3 and SP4, and follows them to step SP5.
[0046]On the other hand, when a negative result is obtained in step SP2, he expresses that this does not have a value of the register MR equal to a broadcast address, i.e., the packet concerned is not a broadcasting packet, and follows the decoding part 34 to step SP3.
[0047]In step SP3, in the key table 37, while a Valid bit is "1" (namely, effective state), the decoding part 34, Based on (1) type, each line search of the key table is carried out from #1 line at order for whether a line with equal register MR and MAC Address exists in all the bits of the section whose mask bit is "1."
[0048]When an affirmation result is obtained in step SP3, this means that a line with equal register MR and MAC Address existed in all the bits of the section an effective state and whose mask bit are "1", and he follows the decoding part 34 to step SP5.
[0049]On the other hand, when a negative result is obtained in step SP3, this means that a line with equal register MR and MAC Address does not exist in all the bits of the section an effective state and whose mask bit are "1", and he follows the decoding part 34 to SUTE 4.
[0050]In step SP4, the decoding part 34 generates a hash value from a MAC Address of a statement to a packet header using a hash function, searches a predetermined hash table using the hash value concerned, and judges whether a bit corresponding to a hash value is "1."
[0051]When a negative result is obtained in step SP4, bit of this of a hash table is "0", It expresses that the packet concerned is not a packet which the receiving set 21 should receive, and it progresses to step SP13, and the decoding part 34 cancels the packet concerned, and ends processing by step SP14.
[0052]On the other hand, when an affirmation result is obtained in step SP4, bit of this of a hash table is "1", and he expresses that the packet concerned is a packet which the receiving set 21 should receive, and follows the decoding part 34 to step SP5.
[0053]In step SP5, the decoding part 34 judges whether the packet concerned is enciphered based on a value of a lower bit of PSC (Payload Scrambling Control) (drawing 3) in a packet header. When a negative result is obtained in step SP5, lower

bit of this should be "0." That is, it means that the packet concerned is not enciphered, and it progresses to step SP14 and the decoding part 34 ends sending processing for a packet to the latter checker 35, without performing code release processing.

[0054]On the other hand, when an affirmation result is obtained in step SP5, this expresses that a lower bit is "1", i.e., the packet concerned is enciphered, and he follows the decoding part 34 to step SP6.

[0055]In step SP6, the decoding part 34 judges whether the packet concerned is enciphered using a common key based on a value of CKI (drawing 3) in a packet header. CKI of this should be "0" when an affirmation result is obtained in step SP6. Namely, it means that the packet concerned is enciphered using a common key, and he progresses to step SP7, and the decoding part 34 substitutes "1" which shows a common key to the register k which memorizes an index number of a key, and follows it to step SP10.

[0056]On the other hand, when a negative result is obtained in step SP6, this expresses that CKI is "1", i.e., the packet concerned is enciphered using an individual key, and he follows the decoding part 34 to step SP8.

[0057]In step SP8, the decoding part 34 order-of-rows-next[each]-searches a key table based on (1) type, and it is judged whether a MAC Address corresponding to MR exists on a key table. A packet which should not receive will also make it pass by discrimination by a hash table in step SP4 here, if a hash value agrees by chance, but since it is again discriminated in the step SP8 concerned, decoding processing of such a packet is not carried out accidentally. Since a packet which is not enciphered incidentally does not pass step SP8, this is canceled with a latter-part circuit or the information processor 22.

[0058]Search of a key table is performed sequentially from the 1st line of the key table concerned, and collation is repeated until it agrees first. A Valid bit indicated to be an effective address to drawing 5 here is an active state. For example, if a Valid bit makes a state of "1" an active state, information on a line that a Valid bit is "0" will become invalid. For example, these values are not referred to whatever it may be set as K_{2Even} and K_{2Odd} that a Valid bit of MAC Address #2 is "0."

[0059]When a negative result is obtained in step SP8, a MAC Address with which this agrees in MR does not exist on a key table, It expresses that the packet concerned is not a packet which the receiving set 21 should receive, and it progresses to step SP13, and the decoding part 34 cancels the packet concerned, and ends processing by step SP14.

[0060]On the other hand, when an affirmation result is obtained in step SP8, a MAC Address with which this agrees in MR exists on a key table, It expresses that the packet concerned is a packet which the receiving set 21 should receive, and he progresses to step SP9, a MAC Address substitutes for the register k an index

number of a key which agreed under conditions of (1) type, and the decoding part 34 follows it to step SP10.

[0061]In step SP10, the decoding part 34 judges that which is enciphered [whether the packet concerned is enciphered with a key of an Even period, and] with a key of an Odd period based on a high order bit of PSC. For example, when a high order bit of PSC is "0", an Even period and in the case of "1", it is determined that it is an Odd period.

[0062]And when a high order bit of PSC of the decoding part 34 is "0", Take out a value of a key of an Even period corresponding to MAC Address #i which agreed, and a Valid bit of K_{iEven} from a key table, and when a high order bit of PSC is "1", A value of a key of an Odd period corresponding to MAC Address #i which agreed, and a Valid bit of K_{iOdd} is taken out from a key table, and it progresses to the following step SP11.

[0063]In step SP11, the decoding part 34 judges whether or a value of a taken-out Valid bit is "1" (namely, Valid(k, EO) =1), it is. When a negative result is obtained in step SP11, Valid (k, EO) of this should be "0." That is, in spite of enciphering a packet, it means that an effective decode key (individual key) does not exist, and it progresses to step SP13, and the decoding part 34 cancels the packet concerned, and ends processing by step SP14.

[0064]On the other hand, when an affirmation result is obtained in step SP11, this expresses that Valid (k, EO) is "1", i.e., an effective decode key (individual key) to a packet exists, and he follows the decoding part 34 to step SP12.

[0065]In step SP12, the decoding part 34 picks out a decode key corresponding to KEY (k, EO), i.e., EO of No. k, from the key table 37, decodes a packet using the decode key concerned, outputs it to the latter checker 35, and ends processing by step SP14.

[0066]The decoding part 34 performs packet decoding processing corresponding to each distribution gestalt of a unicast, multicasting, and broadcasting based on the key table 37 and a hash table in this way.

[0067]Here, since retrieval processing (Steps SP5-SP13) of a decode key in this decoding processing is processed independently of a discrimination process (Steps SP1-SP4) of a MAC Address, it can perform encryption processing also to a broadcast address. In this case, two common key setting methods, the 1st method of using a common key as a communicative decode key to a broadcast address and the 2nd method of registering a broadcast address to a key table as a MAC Address corresponding to an individual key, can be considered.

[0068]In the 1st method, although a storage area of the key table 37 is not consumed, it must share other simultaneous transmissive communication and keys. By the 2nd method, although a storage area of a key table is consumed, a decode key only for broadcasting can be set up.

[0069](5) In operation in an embodiment, and composition beyond an effect the

decoding part 34, While discriminating from a packet which has a broadcast address ("0xFFFFFFFFFFFF") based on a MAC Address described by each packet of the data stream D31 which received, A MAC Address using a mask bit is compared and it discriminates from a packet of multicasting and a unicast. At this time, the decoding part 34 computes a hash value of a MAC Address, and performs packet discrimination of multicasting and a unicast based on the hash value concerned.

[0070]And when it detects whether a packet from which it was discriminated is enciphered and the packet concerned is enciphered, the decoding part 34 picks out a decode key from a key table, and performs decoding processing. At this time, the decoding part 34 distinguishes what encryption of the packet concerned depends on a common key, or a thing to depend on an individual key based on CKI of a packet, and decodes a packet using a common key or an individual key according to this.

[0071]While using a specific MAC Address as a broadcast address according to the above composition, By having compared only some bits of a MAC Address using a mask bit, various reception controls, such as broadcasting, multicasting, and a unicast, can be performed.

[0072]Circuit structure of the decoding part 34 is reducible by reducing the number of bits of a MAC Address using a hash function, and having been made to discriminate from a packet using the reduced MAC Address concerned.

[0073](6) In other embodiments, in addition above-mentioned embodiments, although a bit of a position whose mask bit is "1" was made into a comparison object of a MAC Address, this invention may be made to make a bit of not only this but a position whose mask bit is "0" conversely a comparison object of a MAC Address.

[0074]In an above-mentioned embodiment, in discrimination of a packet using a hash table, when search results of a hash table were "0", canceled a packet, but. This invention may set up a hash table cancel a packet not only this but when search results of a hash table are "1" conversely.

[0075]In a further above-mentioned embodiment, although MAC Address"0xFFFFFFFFFFFF" was made into a broadcast address, this invention is good also considering MAC Address"0xFFFFFFFFFFFF" not only this but other than this as a broadcast address.

[0076]In a further above-mentioned embodiment, although it was made to process in order of collation (step SP3) of a MAC Address in discrimination (step SP2) of a broadcast address, and a key table, and search (step SP4) of a hash table in decoding processing, This invention may be made to perform decoding processing in order not only this but other than this.

[0077]In a further above-mentioned embodiment, although a case where this invention was applied to satellite data transmission systems was described, this invention may be applied to data transmission systems not only this but other than this, for example, cable Internet etc.

[0078]

[Effect of the Invention]When transmitting data individually to a receiving set as mentioned above, while according to this invention giving an address peculiar to the receiving set concerned to the data concerned and transmitting, The common address information which expresses the intersection of the address which is common between the receiving sets of the arbitrary groups concerned when transmitting common data to arbitrary groups' receiving set, While giving the address range information which specifies the range of the intersection of the address concerned to the data concerned and transmitting, When the transmitted data is received and a peculiar address and the address given to the data concerned are in agreement, Or when a peculiar address is compared with the common address information given to the data concerned in the range which address range information shows and a comparison result is in agreement, various reception controls can be performed with simple composition by having decoded the data concerned.

DESCRIPTION OF DRAWINGS

[Brief Description of the Drawings]

[Drawing 1]It is a block diagram showing the entire configuration of the satellite data transmission systems by this invention.

[Drawing 2]It is a block diagram showing the circuitry of a receiving set.

[Drawing 3]It is an approximate line figure showing a header format.

[Drawing 4]It is an approximate line figure showing the relation between a mask and a MAC Address.

[Drawing 5]It is an approximate line figure showing the data configuration of a key table.

[Drawing 6]It is a flow chart which shows decoding processing.

[Description of Notations]

1 .... Satellite data transmission systems, 2 .... A transmitting side system, 3 .... Satellite, 4 .... A receiving system, 5 .... The Internet, 10 .... Control device, 11 .... A digital service unit, 12 .... A data server, 13 .... Transmitting processing unit, 14 .... A local network, 15 .... A transmission antenna, 20 .... Receiving antenna, 21 .... A receiving set, 22 .... An information processor, 23 .... Digital service unit, 24 [.... A demultiplexer, 33 / .... A receiving filter, 34 / .... A decoding part, 35 / .... A checker, 36 / .... A buffer, 37 / .... A key table, 38 / .... An interface part, 39 / .... Bus.] .... A local network, 30 .... CPU, 31 .... A front end section, 32